7K

УДК 519.22; 004.415.24

Н.В. Кошкіна
Інститут кібернетики імені В.М. Глушкова НАН України, м. Київ
Україна, 03680, м. Київ, пр. Академіка Глушкова, 40

Стеганоаналіз МІК-стеганографії на базі матриці суміжності та методу опорних векторів

N.V. Koshkina
V.M. Glushkov Institute of Cybernetics NAS of Ukraine, Kyiv
Ukraine, 03680, Kyiv, Glushkova ave., 40

Steganalysis of QIM-Steganography Based on Co-Occurrence Matrix and the Support Vector Machine

Н.В. Кошкина
Институт кибернетики имени В.М. Глушкова НАН Украины, г. Киев
Украина, 03680, г. Киев, пр. Академика Глушкова, 40

Стеганоанализ МИК-стеганографии на основе матрицы смежности и метода опорных векторов

Розглянуто підхід до стеганоаналізу МІК-стеганографії, що ґрунтується на використанні рядків матриці суміжності як характеристичних векторів аудіосигналів, чуттєвих до процесу вкраплення таємного повідомлення. А також використанні бінарного класифікатора, який реалізує метод опорних векторів та задіяний для розрізнення пустих та стеганоконтейнерів. Досліджено ефективність представленого підходу при різних параметрах стеганоперетворення.
Ключові слова: інформаційна безпека, стеганографія, стеганоаналіз, аудіосигнали, матриця суміжності, метод опорних векторів.

The approach to steganalysis of QIM steganography is considered. It is based on feature vectors of audio signals derived from co-occurrence matrix in time domain, which is sensitive to data embedding process. It also uses the binary classifier that implements the support vector machine and is used for separation of empty and stego containers. The efficiency of this approach wis investigated with using of various parameters of stego transformation.
Key words: information security, steganography, steganalysis, audio signals, co-occurrence matrix, SVM.

Рассмотрен подход к стеганоанализу МИК-стеганографии, базирующийся на использовании строк матрицы смежности в качестве характеристических векторов аудиосигналов, чувствительных к процессу внедрения секретного сообщения. А также использовании бинарного классификатора, который реализует метод опорных векторов и задействован для различения пустых и заполненных контейнеров. Исследована эффективность представленного подхода при различных параметрах стеганопреобразования.
Ключевые слова: информационная безопасность, стеганография, стеганоанализ, аудиосигналы, матрица смежности, метод опорных векторов.

Вступ

Стеганоаналіз є пасивною атакою на стеганографічні системи. Він не змінює вміст атакованих сигналів чи зображень, але виявляє наявність в них прихованих повідомлень та в деяких випадках їх об'єм чи зміст. В стеганоаналітичних дослідженнях широко використовується апарат теорії ймовірностей та математичної статистики, статистичного

аналізу, лінійної алгебри, комбінаторики, цифрової обробки та розпізнавання сигналів і зображень, а також інші розділи математики [1].

Якість стеганоаналітичного методу в цілому може бути оцінена за наступними показниками: ефективність, придатність, практичність та складність. Ефективність відображає точність розрізнення пустих та стеганоконтейнерів. При розрізненні можливе виникнення помилок двох типів: прийняття пустого контейнера за заповнений – хибно позитивна тривога, та прийняття заповненого контейнера за пустий – хибно негативна тривога. Вірогідність виникнення обох типів помилок повинна бути мінімізована. Придатність вимірюється кількістю стеганографічних перетворень, які здатен виявити даний метод стеганоаналізу. Практичність оцінюється широтою сфери практичного застосування методу, можливостями його автоматизації та роботи в реальному режимі часу. Складність є показником необхідних для реалізації програмно-апаратних ресурсів та їх вартості.

У даній статті представлено один з підходів до стеганоаналізу аудіосигналів, що використовує метод опорних векторів, який класифікує тестові сигнали як пусті чи заповнені контейнери залежно від значень рядків матриці суміжності цих сигналів. Ефективність такого підходу перевірялася на одному з класичних методів аудіостеганографії – модуляції індексу квантування (МІК) [2-4], а його реалізація та тестування були виконані за допомогою математичного пакету Matlab.

Метою даної роботи є дослідження ефективності представленого стеганоаналітичного методу та його придатності для стеганоаналізу МІК-стеганографії при зміні сили та кроку вкраплення.

Метод модуляції індексу квантування

Нехай $m_k \in \{0,1\}$ – k-й біт таємного повідомлення; $f(k)$ – вихідне значення відліку аудіосигналу, що слугуватиме носієм даного біту; $f'(k)$ – результат квантування, тобто відповідний відлік стеганосигналу; S – сила вкраплення.

Схематично принцип дії МІК представлений на рис. 1.

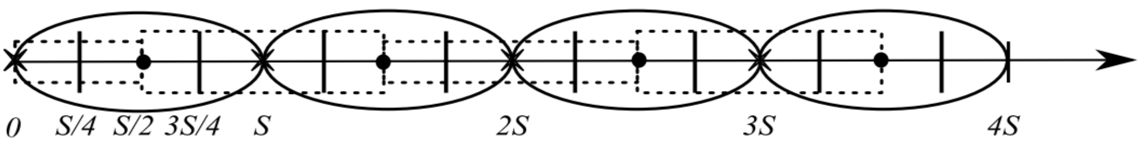


Рисунок 1 – Схема модуляції індексу квантування

В стеганоперетворенні беруть участь два квантувача, використання першого з них відповідає вкрапленню одиничного біта, другого – нульового біта. Так, на рис. 1 еліпсами позначені інтервали квантування першого квантувача, крапки в центрі кожного еліпса – точки квантування першого квантувача. Якщо $m_k = 0$ і $f(k)$ знаходиться в межах деякого еліпсу, перший квантувач ставить у відповідність $f'(k)$ значення, що відповідає значенню точки в центрі даного еліпсу. Аналогічно прямокутниками, намальованими штриховою лінією, позначені інтервали квантування другого квантувача, а знаком «×» – його точки квантування. Якщо $m_k = 1$ і $f(k)$ знаходиться в межах деякого прямокутника, другий квантувач ставить у відповідність $f'(k)$ значення, що відповідає значенню точки в центрі даного прямокутника. При цьому крок квантування обох квантувачів $\Delta = S$.

При вилученні повідомлення декодер порівнює відстань від $f''(k)$ – поточної точки прийнятого сигналу, до кожної з найближчих точок квантування, які позначені «•» та «×», якщо $f''(k)$ ближче до «•» – вилучається нульовий біт, ближче до «×» –

вилучається одиничний. Межі між значеннями, що відповідають 0 або 1 при декодуванні на рис. 1 позначені вертикальними лініями.

Таким чином, формула для вкраплення біту повідомлення буде такою:

$$f'(k) = \begin{cases} floor\left(\dfrac{f(k)}{S}\right) \cdot S + \dfrac{S}{2}, & \text{якщо } m_k = 0, \\ round\left(\dfrac{f(k)}{S}\right) \cdot S, & \text{якщо } m_k = 1, \end{cases} \tag{1}$$

де *round*(*x*) означає операцію округлення до найближчого цілого числа; *floor*(*x*) – операцію округлення зі сторони мінус нескінченності.

Наступна формула використовується для вилучення біту повідомлення:

$$m'_k = \begin{cases} 0, & \text{якщо } \dfrac{S}{4} \le mod\,(f''(k), S) < \dfrac{3S}{4}, \\ 1, & \text{у інших випадках}. \end{cases} \tag{2}$$

Тут *mod*(*x*,*y*) – це залишок від ділення *x* на *y*.

Аналіз невідчутності. Оцінка невідчутності для МІК може бути представлена як значення середньоквадратичної похибки після вкраплення даних:

$$D(f'(k), f(k)) = \frac{1}{N} \sum_{k=1}^{N} \left(f'(k) - f(k)\right)^2, \tag{3}$$

де N – кількість бітів прихованого повідомлення.

Якщо крок квантування Δ є досить маленьким, $f(k)$ можна представити рівномірно розподіленим в межах кожного інтервалу квантування. В цьому випадку рівність (3) може бути промодельована як

$$D(f'(k), f(k)) = \frac{1}{\Delta} \int_{-\frac{\Delta}{2}}^{\frac{\Delta}{2}} u^2 du = \frac{\Delta^2}{12}. \tag{4}$$

Рівність (4) показує, що спотворення, які привносяться вкрапленням, знаходяться у пропорції до квадрату кроку квантування. Тобто, невідчутність залежить тільки від кроку квантування та не залежить від сигналу. Але коли $f(k)$ приймає маленькі значення, співвідношення сигнал/шум після квантування виявляється низьким та спотворення привнесені маркуванням в цих випадках можуть бути відчутними на слух.

Визначення чутливих до МІК характеристик сигналу

При обчисленні текстурних характеристик зображень широко використовується напівтонова матриця суміжності (GLCM – gray level co-occurrence matrix) – гістограма другого порядку, що показує ймовірність сумісної появи певних значень пікселів на заданій відстані та в певному напрямі [5]. Подібну характеристику можна побудувати й для аудіосигналів. Для деякого аудіосигналу $f(k)$ його матриця суміжності визначається як:

$$P(\Delta d, d) = \#\left\{ k \mid (d-1) \cdot \Delta d < \left| f(k+d) - f(k) \right| \le d \cdot \Delta d \right\}. \tag{5}$$

Тут # позначена кількість пар відліків аудіосигналу, для яких різниця амплітуд лежить в межах від $(d-1) \cdot \Delta d$ до $d \cdot \Delta d$, d – інтервал затримки за часом між відліками в парі, Δd – фіксована роздільна здатність аналізу сумісної появи значень відліків.

Так як стеганографічне приховання даних не повинне вносити відчутних шумів в оригінальний контейнер, є певні обмеження зверху на величину привнесених вкрапленням

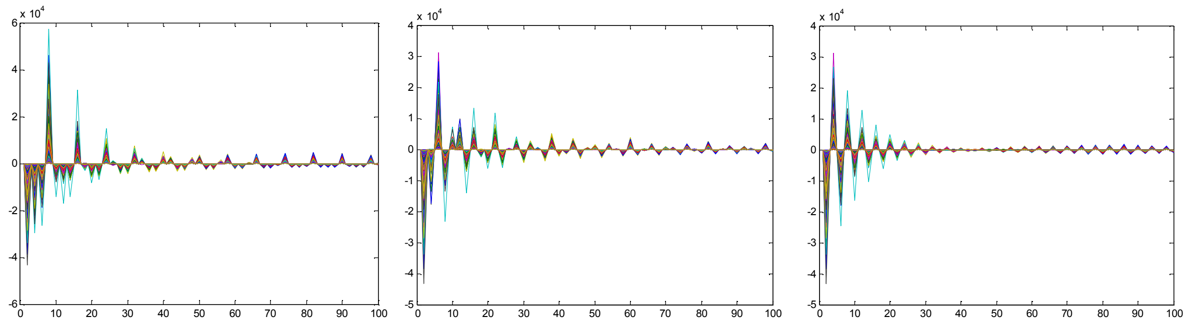
спотворень вихідних відліків. Отже, можна очікувати, що стеганографічне перетворення сигналу буде більш вливати на значення його матриці суміжності для порівняно малих *d*.

Щоб прослідкувати, як стеганографічне перетворення, в даному випадку МІК, впливає на матрицю суміжності аудіосигналів, було обрано понад тисячу 10-секундних фрагментів аудіокниг у форматі *.wav(pcm) з частотою дискретизації 44 кГц та розрядністю квантування 16 біт. З них за допомогою МІК з різними кроками квантування було отримано набори стеганосигналів. Відмітимо, що аудіосигнал, який в Matlab зчитується функцією *wavread*, за замовчуванням нормується до одиниці, і сила вкраплення повинна бути приведена у відповідність до масштабу сигналу.

В подальшому було обчислено рядки матриць суміжності оригінальних та стеганосигналів для різних малих Δd . А потім розглянуто різниці між відповідними рядками, що отримані з пустих та заповнених контейнерів:

$$G_{\Delta d} = P_{orig}(\Delta d, d) - P_{stego}(\Delta d, d), \;\; d = 1,2\ldots100.$$

Так, на рис. 2 а-в) наведені графіки цих різниць при $\Delta d = 2^{-16}$. Емпірично ця роздільна здатність виявилася найкращою для відслідковування розбіжностей в матрицях суміжності пустих та заповнених контейнерів.



а) $S = \frac{1}{4}\cdot 10^{-3}$ б) $S = \frac{1}{6}\cdot 10^{-3}$ в) $S = \frac{1}{8}\cdot 10^{-3}$

Рисунок 2 – Різниці векторів суміжності оригінальних та стеганосигналів

Як бачимо, після вкраплення таємного повідомлення рядки матриці суміжності змінюються, в цих змінах простежуються чіткі закономірності, а особливо сильні зміни, як і передбачалося спостерігаються для порівняно малих *d*. Таким чином, матриця суміжності є чуттєвою до стеганографічних перетворень, згідно з методом МІК, характеристикою аудіосигналу, дані якої, отримані при коректно підібраних параметрах розрахунку, можна використовувати як основу для розрізнення пустих та заповнених контейнерів.

Класифікація сигналів за методом опорних векторів

Після того як визначено набори характеристичних векторів для пустих та заповнених аудіосигналів, потрібен ефективний бінарний класифікатор. Один з таких класифікаторів – метод (машина) опорних векторів (SVM – support vector machine). Цей метод відноситься до граничних методів класифікації та широко використовується при розв’язанні задач стеганоаналізу [6-8]. Крім стеганоаналізу його використовують в багатьох прикладних областях, зокрема при розпізнаванні образів, ідентифікації диктора, класифікації текстів, аналізі ДНК, білків та ін. Метод опорних векторів дозволяє отримати функцію класифікації з мінімальною верхньою оцінкою рівня похибки класифікації, а також використовувати лінійний класифікатор для роботи з лінійно нероздільними даними.

Нехай маємо навчальну вибірку $(X,t)=\{\vec{x}_n,t_n\}_{n=1}^{N}$, де $\vec{x}_n$ – деякий об’єкт в просторі R^n, $t_n \in \{-1,+1\}$ – його мітка класу. Задача полягає в тому, щоб на основі навчальної вибірки спрогнозувати мітку класу $\hat{t}$ для нового об’єкту $\vec{x}$.

В нашому застосуванні $\vec{x}_n$ може бути певним характеристичним вектором, вилучений з аудіосигналу, зокрема рядком матриці суміжності, що обчислюється за формулою (5). Якщо $\vec{x}_n$ вилучено з пустого контейнера, то $t_n=-1$, якщо з заповненого, то $t_n=+1$.

Лінійний класифікатор

Для лінійної SVM ми шукаємо лінійну функцію прийняття рішень

$$p(\vec{x})=sign(\vec{w}\cdot\vec{x}-b).$$

З погляду геометрії лінійний класифікатор відповідає деякій поділяючій гіперплощині, де об’єкт відноситься до першого класу, якщо він лежить з додатної сторони від гіперплощини, та до другого в протилежному випадку. Вектор $\vec{w}$ є перпендикуляром до поділяючої гіперплощини, а параметр b визначає її зсув відносно початку координат.

Розглянемо випадок коли навчальна вибірка (X,t) є лінійно роздільною. Провести гіперплощину, поділяючу об’єкти на класи, можна по-різному. Разом з тим оптимальною є така гіперплощина, яка максимізує відстань між нею та найближчим об’єктом класу. Гіперплощину будемо називати опорною для множини об’єктів, якщо всі об’єкти лежать по одну сторону від неї. Поділяючу гіперплощину можна побудувати таким чином: знайти дві паралельні опорні гіперплощини для об’єктів двох класів, а потім на рівних відстанях від них провести третю паралельну гіперплощину (рис. 3 а). Поділяюча гіперплощина буде оптимальною при максимальній ширині смуги між опорними гіперплощинами. Таким чином, маємо задачу квадратичної оптимізації:

$$\begin{cases}\dfrac{2}{\|\vec{w}\|}\to\max\limits_{\vec{w},b},\\ \vec{w}\cdot\vec{x}_n-b\ge 1,\ \text{при}\ \ t_n=1,\\ \vec{w}\cdot\vec{x}_n-b\le -1,\ \text{при}\ \ t_n=-1,\end{cases}\Leftrightarrow\begin{cases}\dfrac{1}{2}\|\vec{w}\|^2\to\min\limits_{\vec{w},b},\\ t_n\left(\vec{w}\cdot\vec{x}_n-b\right)\ge 1.\end{cases}\tag{6}$$

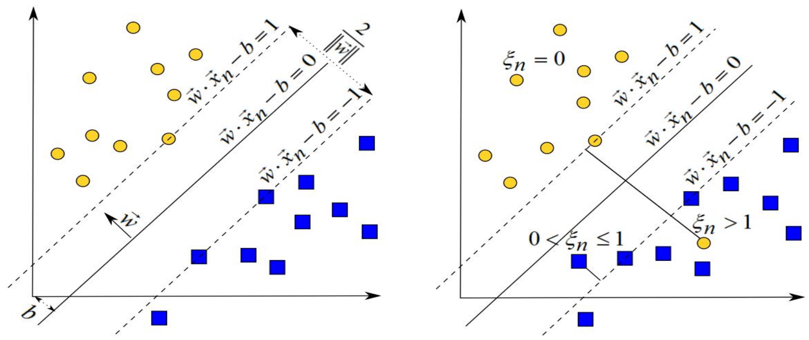
Через складність обмежень безпосередній розв’язок цієї задачі є складним. Для її спрощення використовують метод Лагранжа. Щоб знайти розв’язок, необхідно сформулювати двоїсту задачу, в якій з кожним обмеженням $t_n\left(\vec{w}\cdot\vec{x}_n-b\right)\ge 1$ прямої задачі зв’язаний відповідний множник Лагранжа α_n. Двоїста до (6) задача оптимізації має вигляд:

$$\begin{cases}\sum\limits_{i=1}^{N}\alpha_i-\dfrac{1}{2}\sum\limits_{i=1}^{N}\sum\limits_{j=1}^{N}\alpha_i\alpha_j t_i t_j\vec{x}_i\cdot\vec{x}_j\to\max\limits_{\alpha},\\ \alpha_i\ge 0,\ \ 1\le i\le N,\\ \sum\limits_{i=1}^{N}\alpha_i t_i=0.\end{cases}\tag{7}$$

Розв’язком (7) буде $\vec{w}=\sum\limits_{i=1}^{N}\alpha_i t_i\vec{x}_i$. Для більшості векторів $\alpha_i=0$. Всі вектори, для яких $\alpha_i>0$ називають опорними. Для будь-якого опорного вектору $b=\vec{w}\cdot\vec{x}_i-t_i$, тобто він належить опорній гіперплощині.

Таким чином, функція прийняття рішень матиме вигляд:

$$p(\vec{x}) = sign(\sum_{i=1}^{N} \alpha_i t_i \vec{x}_i \cdot \vec{x} - b)\,. \tag{8}$$



а) hard-margin SVM б) soft-margin SVM

Рисунок 3 – Побудова оптимальної поділяючої гіперплощини

Розглянемо випадок довільних даних. Коли дані є лінійно нероздільними, умови $t_n(\vec{w} \cdot \vec{x}_n - b) \ge 1$ не можуть бути виконаними для всіх об'єктів. Тоді в ці умови додають послаблюючі коефіцієнти $\xi_n \ge 0$:

$$t_n(\vec{w} \cdot \vec{x}_n - b) \ge 1 - \xi_n\,.$$

Якщо $\xi_n = 0$, то для об'єкта $\vec{x}_n$ помилки немає, він лежить за опорною гіперплощиною свого класу $|p(\vec{x})| = 1$. Якщо $0 < \xi_n \le 1$, помилки немає, об'єкт лежить всередині поділяючої смуги $0 \le t_n p(\vec{x}) < 1$. Якщо $\xi_n > 1$, помилка є, її величина пропорційна відстані від об'єкта до опорної гіперплощини його класу (рис. 3 б).

Модифікуємо критерій оптимізації в задачі (6), включивши до нього число помилок у вибірці:

$$\begin{cases} \frac{1}{2}\|\vec{w}\|^2 + C\sum_{n=1}^{N} \xi_n \to \min\limits_{\vec{w},b,\xi}, \\ t_n(\vec{w} \cdot \vec{x}_n - b) \ge 1 - \xi_n, \\ \xi_n \ge 0. \end{cases} \tag{9}$$

Тут $C \ge 0$ – коефіцієнт регуляризації, що визначає компроміс між числом помилок на навчальній вибірці та простотою лінійної функції прийняття рішень.

Таким чином для довільних даних метод опорних векторів полягає в побудові поділяючої гіперплощини за допомогою розв'язку задачі оптимізації (9). Ця задача квадратичної оптимізації, як і в попередньому випадку, зводиться до задачі для множників Лагранжа:

$$\begin{cases} \sum_{i=1}^{N} \alpha_i - \frac{1}{2}\sum_{i=1}^{N}\sum_{j=1}^{N} \alpha_i \alpha_j t_i t_j \vec{x}_i \cdot \vec{x}_j \to \max\limits_{\alpha}, \\ 0 \le \alpha_i \le C,\ 1 \le i \le N, \\ \sum_{i=1}^{N} \alpha_i t_i = 0. \end{cases}$$

На практиці для побудови машини опорних векторів розв'язують саме цю задачу, а не (7), так як в загальному випадку гарантувати лінійну роздільність не можна. Цей варіант алгоритму називають алгоритмом з м'яким краєм (soft-margin SVM), тоді як в лінійно роздільному випадку говорять про жорсткий край (hard-margin SVM). Функція прийняття рішень зберігає вигляд (8), але тепер ненульові α_i мають не тільки опорні об'єкти, а й об'єкти-порушники. В певному сенсі це є недоліком, оскільки порушниками часто стають шумові викиди та функція прийняття рішень по суті буде опиратися на шум. Тому якщо відомо, що вибірка майже лінійно роздільна, доцільно виконати фільтрацію викидів.

Нелінійний класифікатор

Існує ще один шлях до вирішення проблеми лінійної нероздільності: вихідний простір R^n можна відобразити в простір більш високого розміру, де навчальна вибірка стане лінійно-роздільною $\Phi : \vec{x} \to \phi(\vec{x})$. Цей простір називають спрямляючим (рис. 4).

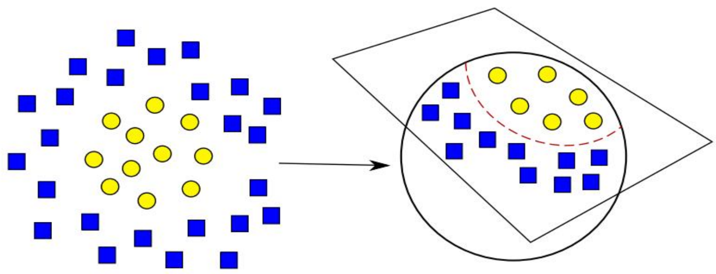


Рисунок 4 – Відображення навчальної вибірки в простір більш високого розміру

Об'єкти навчальної вибірки входять в лінійну функцію прийняття рішень тільки у вигляді попарних скалярних добутків $\vec{x}_i \cdot \vec{x}_j$. Отже, для того, щоб побудувати оптимальну поділяючу гіперплощину в новому просторі, необхідно знати лише $\phi(\vec{x}_i)\cdot\phi(\vec{x}_j)$. Припустимо, що існує деяка функція $K : R^n \to R$, така що $K(\vec{x}_i, \vec{x}_j) = \phi(\vec{x}_i)\cdot\phi(\vec{x}_j)$. Тоді для побудови оптимальної поділяючої гіперплощини не обов'язково задавати перетворення Φ в явному вигляді, достатньо лише знати K. При цьому функцію прийняття рішень (8) можна переписати як

$$p(\vec{x}) = sign(\sum_{i=1}^{N} \alpha_i t_i K(\vec{x}_i, \vec{x}) - b)\,. \qquad (10)$$

Такий підхід називають переходом до ядра (kernel trick). Ядро K – це функція, що відповідає скалярному добутку в деякому спрямляючому просторі. Для того щоб відповідна задача квадратичного програмування мала розв'язок, воно повинне задовольняти умові Мерсена:

$$\int K(\vec{x}, \vec{y}) g(\vec{x}) g(\vec{y}) d\vec{x} d\vec{y} \ge 0 \quad \forall g(\vec{x}) : \int g^2(\vec{x}) d\vec{x} < \infty\,.$$

Ядро K повинне бути неперервним, симетричним та мати позитивно визначену матрицю Грама.

SVM в математичному пакеті Matlab реалізовано функцією *svmtrain*. Серед її вхідних аргументів є *'kernel_function'*, що дозволяє користувачеві задавати наступні ядра:

– *'linear'* – лінійне $K(\vec{x}_i, \vec{x}_j) = \vec{x}_i \cdot \vec{x}_j + \theta, \theta \ge 0$;

– *'quadratic'* – квадратичне $K(\vec{x}_i, \vec{x}_j) = \left(\vec{x}_i \cdot \vec{x}_j + \theta\right)^2, \theta \ge 0$;

– *'polynomial'* – поліноміальне $K(\vec{x}_i, \vec{x}_j) = \left(\vec{x}_i \cdot \vec{x}_j + \theta\right)^d, \theta \ge 0$ (порядок за замовчуванням рівний 3);

– *'rbf'* – Гаусіана $K(\vec{x}_i,\vec{x}_j)=\exp\left(-\frac{\|\vec{x}_i-\vec{x}_j\|}{2\sigma^2}\right), \sigma>0$ (за замовчуванням $\sigma=1$);

– *'mlp'* – багатошаровий перцептрон.

Результати тестування

Тестування описаного підходу виконувалося згідно з наступною схемою (рис. 5).

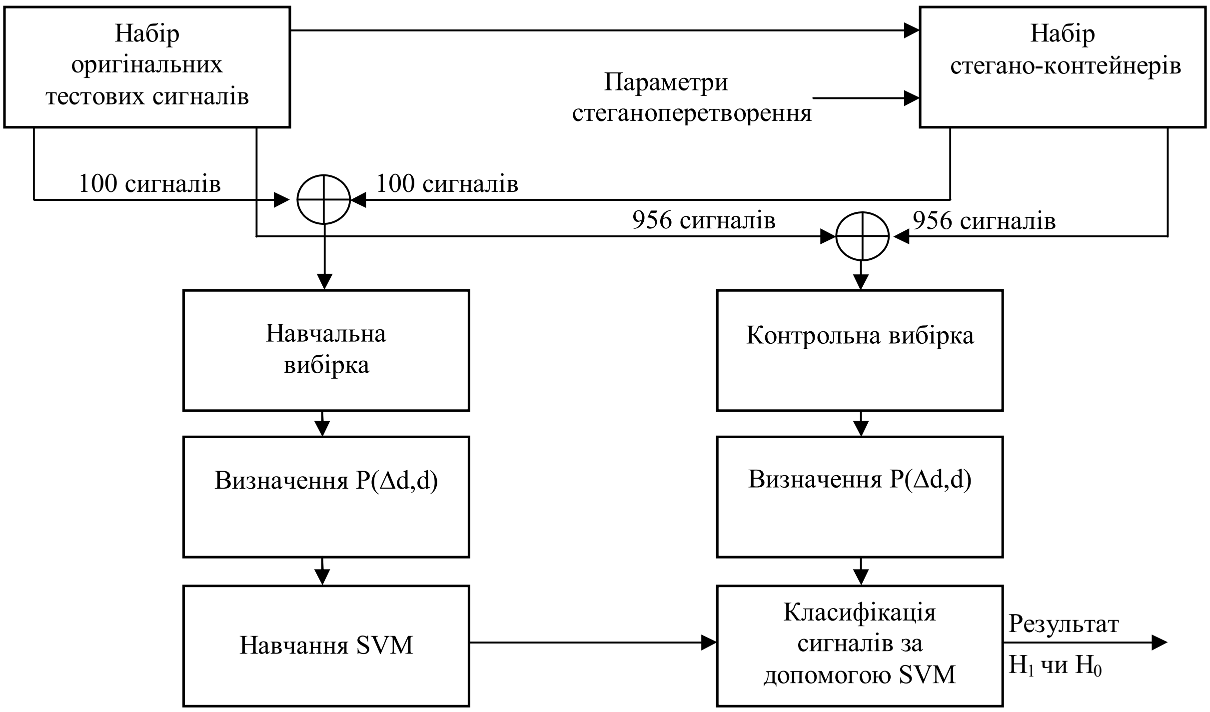


Рисунок 5 – Загальна схема тестування

Навчальна вибірка для функції *svmtrain* складалася з 100 пустих (10-секундні фрагменти аудіокниг) та 100 заповнених контейнерів, отриманих за допомогою методу МІК з різними параметрами вкраплення. Зауважимо, що більш тривалі сигнали можуть бути розділеними на блоки, до кожного з яких застосовується даний підхід. Це дозволить виявляти приховані дані, присутні в частині сигналу-контейнера.

Рядки матриці суміжності сигналів $P(\Delta d, d)$ обчислювалися для $\Delta d = 2^{-16}$. Контрольна вибірка для функції класифікації *svmclassify* містила 956 пустих та 956 заповнених контейнерів, отриманих з такими ж параметрами вкраплення, як і стеганоконтейнери відповідної навчальної вибірки.

Результати

Було виконано тестування для стеганоконтейнерів, отриманих з силою вкраплення $S=\frac{1}{4}\cdot 10^{-3}$ (SNR_{average}=67,25дБ), $S=\frac{1}{6}\cdot 10^{-3}$ (SNR_{average}=70,77дБ), $S=\frac{1}{8}\cdot 10^{-3}$ (SNR_{average}=73,27дБ) та $S=\frac{1}{10}\cdot 10^{-3}$ (SNR_{average}=75,20дБ). При використанні SVM з лінійною функцією ядра для розрізнення пустих та заповнених контейнерів було отримано 100%

коректне спрацьовування, тобто повну відсутність помилок розрізнення. Такий результат має місце і при більших значеннях сили вкраплення, до моменту, коли втручання не стане помітним на слух.

При використанні квадратичного ядра та Гаусіани результати дещо погіршуються, зокрема з ядром Гаусіаною для 12-13% стеганосигналів виникає хибно негативна тривога, а з квадратичним для 2-4% стеганосигналів – хибно негативна і для 0,5% оригінальних сигналів хибно позитивна тривоги. Таким чином для даних умов детектування доцільно використовувати лінійне ядро SVM.

При вкрапленні повідомлення тільки у відліки, амплітуди яких лежать вище певного порогового значення було отримано аналогічні результати тестування. Тобто підхід спрацьовує при використанні порогів, за якими з області вкраплення вилучаються ділянки незначної енергії та тиші.

При 50% послідовному заповненні контейнера зменшується розбіжність між $P_{orig}(\Delta d, d)$ і $P_{stego}(\Delta d, d)$, але разом з тим результати тестування аналогічні результатам при 100%.

Метод виявляє наявність прихованої інформації у випадку, коли для формування тестового набору стеганосигналів використовується різний рівномірний крок вкраплення. Наприклад, в експерименті коли стеганосигнали були сформовані з кроками від 1 до 10 та $S = \frac{1}{8} \cdot 10^{-3}$ було отримано 84,73% коректних спрацьовувань, 6,17% хибно позитивних та 24,37% хибно негативних тривог.

При вкрапленні даних з однаковим рівномірним кроком для всіх стеганосигналів результати розрізнення погіршуються зі збільшенням кроку. Зокрема залежність результатів від кроку вкраплення для МІК з $S = \frac{1}{8} \cdot 10^{-3}$ і використання представленого стеганоаналітичного підходу з лінійним ядром SVM наведена в таблиці 1.

Метод здатен виявляти МІК при розподіленому вкрапленні приховуваних бітів по контейнеру з псевдовипадковим кроком вкраплення. Наприклад, в ході експериментів де крок вкраплення є псевдовипадковою рівномірно розподіленою від 1 до 10 величиною для $S = \frac{1}{8} \cdot 10^{-3}$ було отримано 82,37% коректних спрацьовувань, 22,80% хибно позитивних та 12,45% хибно негативних тривог. При тих же умовах для $S = \frac{1}{4} \cdot 10^{-3}$ було отримано 94,67% коректних спрацьовувань, 6,69% хибно позитивних та 3,97% хибно негативних тривог.

Таблиця 1

Крок вкраплення	Хибно позитивна тривога	Хибно негативна тривога	Коректне спрацьовування
1	0%	0%	100%
2	0%	0%	100%
3	0,10%	0,84%	99,53%
4	4,39%	0,10%	97,75%
5	2,82%	1,98%	97,59%
6	3,66%	2,20%	97,07%
7	16,42%	6,60%	88,49%
8	10,36%	7,74%	90,95%
10	16,21%	9,62%	87,08%
20	39,54%	30,96%	64,75%

Результати розрізнення при відносно малій силі вкраплення наведені у таблиці 2 (при 100% послідовому заповненні контейнера). Зауважимо, що сила вкраплення обмежена знизу значенням $S = 2^{-14}$, бо модифікації меншої сили не будуть збережені при запису сигналу в *.wav файл.

Таблиця 2

Сила вкраплення	$\frac{1}{10}\cdot 10^{-3}$	$\frac{1}{11}\cdot 10^{-3}$	$\frac{1}{12}\cdot 10^{-3}$	$\frac{1}{13}\cdot 10^{-3}$	$\frac{1}{14}\cdot 10^{-3}$	$\frac{1}{15}\cdot 10^{-3}$	$\frac{1}{16}\cdot 10^{-3}$
Коректне спрацьовування	100%	99,11%	99,84%	99,74%	99,63%	91,95%	58,42%

За результатами проведених експериментів представлений метод не є ефективним для виявлення НЗБ-стеганографії, що перевірялося для реалізації НЗБ з 100% послідовним заповненням за допомогою пакету Matlab та для випадку формування стеганоконтейнерів з розподіленим вкрапленням за допомогою програми Steghide. Зауважимо, що при $S = 2^{-14}$ для додатних значень відліків метод МІК модифікує значення відліку аудіосигналу аналогічно класичному методу найменшого значущого біту (НЗБ) і для МІК з такою силою вкраплення використовувана схема тестування також дає поганий результат – 48,27% коректних спрацьовувань.

Висновки

Доступ до стеганоперетворення як до «чорного ящика», тобто можливість для деякого набору пустих контейнерів отримати відповідний йому набір стеганограм, суттєво спрощує роботу стеганоаналітика. Як продемонстровано у даній роботі, аналізуючи розбіжність статистики оригінальних та стеганосигналів за деяким критерієм, наприклад, за матрицею суміжності, аналітик може відслідкувати закономірності, які не залежать від вмісту сигналу-контейнера. Це дозволить виявляти факт використання досліджуваного стеганоперетворення в подальшому.

Відносно представленого підходу можна зробити висновок, що він є ефективним для виявлення МІК-стеганографії при послідовному та розподіленому заповненні контейнера з достатньо значною силою вкраплення та наповненістю контейнера, а також при використанні порогів, що вилучають з області вкраплення ділянки незначної енергії та тиші. При використанні розподіленого вкраплення з рівномірним кроком зі збільшенням кроку та відповідно зменшенням наповненості контейнера ефективність методу зменшується.

При зміні параметрів вкраплення стеганосигналів контрольної вибірки відносно навчальної результат розпізнавання, як правило, погіршується. Особливо суттєвим це погіршення є коли сила вкраплення або наповненість контейнера для контрольної вибірки менша за силу вкраплення або наповненість для навчальної.

Література

1. Швидченко И.В. Методы стеганоанализа для графических файлов / Швидченко И.В. // Искусственный интеллект. – 2010. – № 4. – С. 697-705.
2. Chen B. Quantization index modulation: a class of provably good methods for digital watermarking and information embedding/ B. Chen, G.W. Wornell //IEEE Trans. Information Theory. – 2001. – Vol. 47. – P. 1423-1443.
3. Quantization-Based Digital Audio Watermarking in Discrete Fourier Transform Domain / S. Yang, W. Tan, Y. Chen, W. Ma //Journal of Multimedia. – 2010. – Vol. 5, № 2. – P. 151-158.
4. Xiang S. Analysis of D/A and A/D Conversions in Quantization-based Audio Watermarking / S. Xiang, J. Huang // International Journal of Network Security. – 2006. – Vol. 3, № 3. – P. 230-238.

5. Suresh A., Shunmuganathan K. L. Image Texture Classification using Gray Level Co-Occurrence Matrix Based Statistical Features / Suresh A., Shunmuganathan K. L. // European Journal of Scientific Research. – 2012. – Vol.75, № 4. – P. 591-597.
6. Lyu S., Farid H. Steganalysis using color wavelet statistics and one-class support vector machines / Lyu S., Farid H. // Proc. Security, Steganography, and Watermarking of Multimedia Contents. – 2004. – P. 35-45.
7. Liu Q., Sung A., Qiao M. Spectrum Steganalysis of WAV Audio Streams / Liu Q., Sung A., Qiao M. // International Conference on Machine Learning and Data Mining. – 2009. – Vol. 5632. – P. 582-593.
8. Johnson. M., Lyu. S., Farid. H. Steganalysis of Recorded Speech / Johnson. M., Lyu. S., Farid. H.//Proc. SPIE. – 2005. – Vol. 5681. – P. 664-672.

Literatura

1. Shvidchenko I.V. Iskusstvennyj intellekt. 2010. № 4. S. 697-705.
2. Chen B. IEEE Trans. Information Theory. 2001. Vol. 47. P. 1423-1443.
3. Yang S. Journal of Multimedia. 2010. Vol. 5, № 2. P. 151-158.
4. Xiang S. International Journal of Network Security. 2006. Vol.3. № 3. P. 230-238.
5. Suresh A. European Journal of Scientific Research. 2012. Vol.75. № 4. P. 591-597.
6. Lyu S. Proc. Security, Steganography, and Watermarking of Multimedia Contents. 2004. P. 35-45.
7. Liu Q. International Conference on Machine Learning and Data Mining. 2009. Vol. 5632. P. 582-593.
8. Johnson M. Proc. SPIE. 2005. Vol. 5681. P. 664-672.

RESUME

N.V. Koshkina

Steganalysis of QIM-Steganography Based on Co-Occurrence Matrix and the Support Vector Machine

Access to steganographic transformation as to a “black box” that means the possibility for some set of empty containers to get their appropriate set of stego containers significantly simplifies the steganalysis problem. the analyst can track regularities that are not depend on the signal-container content with using analyzing the statistics differences between original and stego signals by some criterion. In future, these regularities will reveal the fact of usage of this steganographic transformation. This paper presents one such approach to audio steganalysis. It includes support vector machine, which classifies test signals as empty or stego containers depending on the values of rows of co-occurrence matrix of these signals. The efficiency of this approach is tested on one of the classical methods of audio steganography, i.e. quantization index modulation (QIM). Implementation and testing are performed using the mathematical package Matlab.

The research aims the analysis of efficiency of presented steganalytic technique and its applicability for steganalysis of QIM-steganography with various embedding power and step.

The technique that is examined in this article is effective on detecting QIM-steganography with consecutive and distributed data embedding into the audio signal if embedding power and occupancy of container are large enough, and also when we use the thresholds that are exclude from the embedding domain of the regions with small energy, and silence. With use of distributed embedding with uniform step the efficiency of this technique decreases if embedding step increases.

When we change stego embedding parameters for generation of the control set of stego-signals relative to training set, the obtained result is usually worse. This deterioration is especially large when the embedding power or occupancy of container for the control set are less than the embedding power or occupancy for the training set.

Стаття надійшла до редакції 05.06.2012.